Method Of Encoding Information Within Directory Files

On An Integrated Circuit Smart Card

Field of the Invention

[001] This invention relates to an improved method of encoding data within an integrated circuit (IC) card and more specifically to an improved method of encoding data within directory files contained within a PKCS15 compatible integrated circuit (IC) smart card.

Background of the Invention

[002] Smart card (SC) technology has allowed for storing of secure information within an integrated circuit card. The secure information is stored in such a format that software keys and certificates are required for authentication purposes before information is retrieved. An encoding standard, known as PKCS15 dictates how these keys and certificates are represented in terms of smart card files and directories. The format securely controls external access to files and directories on the smart card during the process of encoding information, or reading information from the smart card.

[003] The PKCS15 compatible format for a smart card is documented in "PKCS #15 v1.1: Cryptographic Token Information Syntax Standard", RSA Laboratories, December 21, 1999 and incorporated herein by reference. Each smart card must contain an Object Directory File (ODF). This file contains pointers to other directory files, of which, for example when storing cryptographic keys, some are a Private Key Directory File (PrKDF), a Public Key Directory File (PuKDF), a Secret Key Directory File (SKDF), a Certificate Directory File (CDF), and a Data Object Directory File (DODF).

[004] A Private Key Directory File is regarded as a directory of private key identifiers known to the PKCS15 application and typically stores one private key. At least one PrKDF must be present on the smart card containing private keys. In some cases this private key directory file contains cross-reference pointers to authentication objects used to protect access to keys that reside anywhere on the card. If there are private keys corresponding to public keys also residing on the card then the public keys are stored within a Public Key Directory File (PuKDF). Wherein the public keys and the private keys share the same identifier on the card.

[005] At lease one Secret Key Directory File (SKDF) must be present on a smart card containing secret keys. This SKDF contains general key attributes such as labels and identifiers. In some cases the SKDF also contains cross-reference pointers to authentication objects used to protect access to the keys. A Certificate Directory File (CDF) is regarded as a directory of certificates known to the PKCS15 application and at least one CDF must be present on a smart card. The CDF contains certificates or references to certificates. A Data Object Directory File (DODF) is regarded as a directory of data objects other than keys or certificates. At least one DODF must be present on a smart card containing such data objects. These files contain general data object attributes such as identifiers of the application to which the data object belongs and also pointers to the data objects themselves.

[006] Each of the directory files: Private Key, Public Key, Secret Key, Certificate or Data Object, occupy a non volatile array of addressable memory within the smart card. In the prior art method of encoding, pointer addresses are stored in proximity of a starting address of memory allocated to the smart card directory file, and pointer data stored at a fixed pointer data start address within the memory allocated to the smart card directory file. Unfortunately, after the encoding process two non-continuous blocks of unused memory within directory file result due to the placement of the pointer data start address.

[007] It is therefore an object of this invention to provide an improved method of encoding information within smart card directory files such that a single block of unused memory is available within the smart card directory file after encoding and the improved method allowing for downwards compatibility with PKCS15 compatible application.

Summary of the Invention

[008] In accordance with the invention there is provided a method of encoding information within non-volatile memory of a smart card comprising the steps of:

providing a directory file having a start address and an end address within non-volatile storage of a smart card;

providing a data object for storage within the smart card;

storing the data object in at least a last available memory location within the directory file, the last available memory location nearer a start address of the directory file than an earlier stored data object; and

storing pointer data in at least a first available memory location most proximate the start address and between the start address and the end address, the pointer data indicative of a data object location.

[009] In accordance with another aspect of the invention there is provided a method of encoding information within non-volatile memory of a smart card comprising the steps of:

providing a directory file having a start address and an end address within non-volatile storage of a smart card;

providing a data object for storage within the smart card;

storing the data object in at least an available memory location proximate the last available memory location within the directory file, the last available memory location nearer a start address of the directory file than an earlier stored data object; and

storing pointer data in at least an available memory location proximate the start address and between the start address and the end address, the pointer data indicative of a data object location.

[0010] In accordance with yet another aspect of the invention there is provided a smart card comprising:

a directory file having a start address and an end address within non-volatile storage of a smart card;